WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/32 | A1

(11) International Publication Number: WO 97/39553

(43) International Publication Date: 23 October 1997 (23.10.97)

(21) International Application Number: PCT/US97/04025

(22) International Filing Date: 14 March 1997 (14.03.97)

(30) Priority Data:
08/634,068 17 April 1996 (17.04.96) US

(71) Applicant *(for all designated States except US)*: INTEL CORPORATION [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

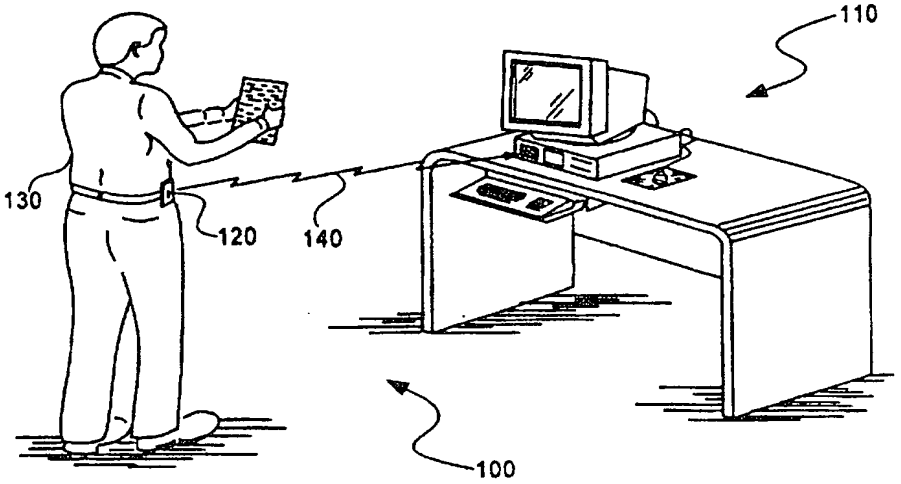
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: DAVIS, Derek, L. [US/US]; 4509 E. Desert Trumpet Road, Phoenix, AZ 85044 (US). SMITH, Lionel [US/US]; 23412 Via del Arroyo, Queen Creek, AZ 85242 (US).

(74) Agents: TAYLOR, Edwin, H. et al.; Blakely, Sokoloff, Taylor & Zafman L.L.P., 1279 Oakmead Parkway, Sunnyvale, CA 94086 (US).

(81) Designated States: AL, AM, AT, AT (Utility model), AU (Petty patent), AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: AN AUTHENTICATION SYSTEM BASED ON PERIODIC CHALLENGE/RESPONSE PROTOCOL



(57) Abstract

A wireless authentication system to control an operating state of a node such as a computer, door control mechanism or any multistate product based on the proximity of an authorized user to the node. The wireless authentication system comprises a security device implemented within the node (110) and a user authentication token ("token") in possession of the authorized user. A Challenge/Response protocol (140) is configured between the security device and the token (120). The first successful Challenge/Response message exchange between the security device and the token (120) places the node (110) in an operational state allowing the authorized user access to the contents and/or networked resources of the node (110). Later Challenge/Response message exchanges are set to occur periodically to check whether the authorized user possessing the token has left the node (110) unattended thereby causing the node (110) to be placed in a non-operational state.

AN AUTHENTICATION SYSTEM BASED ON PERIODIC CHALLENGE/RESPONSE PROTOCOL

CROSS-REFERENCES TO RELATED APPLICATIONS

The named inventor of the present application has filed a number of co-pending United States Patent Applications entitled "Apparatus and Method for Providing Secured Communications" (Application No. 08/578,177), "Secured Method for Providing Secured Communications" (Application No. 08/538,869), "Method For Providing A Roving Software License In A Hardware Agent-Based System" (Application No. 08/472,951), "Key Cache Security System" (Application No. 08/365,347), and "Apparatus and Method for a Vetted Field Upgrade" (Application No. 08/316,211) and issued U.S. Patent entitled "Roving Software License For A Hardware Agent" (U.S. Patent No. 5,473,692). These applications are owned by the same assignee of the present Application.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to data security. More particularly, the present invention relates to a wireless authentication system which mitigates the likelihood of unauthorized use of an electronic device through periodic challenge/response messages.

2. Description of Art Related to the Invention

As personal computers ("PCs") become more prevalent in businesses throughout the world, it is becoming increasingly important to provide security to prevent their unauthorized use.

token cards may be either inserted into a designated card slot of the personal computer, placed in physical contact with a reading device coupled to the computer or placed in an area where the personal computer resides (e.g., an office, laboratory and the like). These token cards are used to verify that the person in possession of the card is in fact authorized to use the personal computer. Depending on the type of token card, such verification is accomplished by the token card responding to a request (i.e., "Challenge message") for information by providing a "token" (i.e. code), normally a random number although it may be static, in response to the challenge issued by the personal computer. In the case of a more sophisticated token card, this request will be in the form of a random "challenge" which the token card must first process in order to provide the correct "response". Although this type of authentication system arguably provides greater security than the password-based system, it still does not solve the problem where the user accesses his or her personal computer and leaves the personal computer unattended for some duration without removing the card or disabling the personal computer during his or her absence.

Hence, it is desirable to develop a wireless authentication system which does not require a physical connection to the personal computer, thereby mitigating the chances of mistakenly leaving one's token card within or in proximity of one's computer. While there now exist some authentication systems in the marketplace such as those provided by Security Dynamics, Inc. of Cambridge, Massachusetts and Digital Pathways of Mountain View, California, their systems do not utilize periodic Challenge/Response protocol to ascertain whether the authorized user of the personal computer has left his or her personal computer unattended for a predetermined period of time.

BRIEF DESCRIPTION OF THE DRAWINGS

The features and advantages of the present invention will become apparent from the following detailed description of the present invention in which:

Figure 1 is a perspective view of the wireless authentication system comprising a personal computer periodically producing a Challenge message to query the proximity of the user and his or her token as well as the token producing a Response message in response to the Challenge message.

Figure 2 is a block diagram of the general architecture of the personal computer of Figure 1.

Figure 3 is a block diagram of an illustrative embodiment of the security device employed within a node as shown in Figure 2.

Figure 4 is a block diagram of an illustrative embodiment of the token of Figure 1.

Figure 5 is a flowchart illustrating the procedural steps undertaken by the wireless authentication system in protecting the integrity of the contents and networked resources of the node through periodic Challenge and Response messages.

Figures 6A-6C are block diagrams of three illustrative embodiments of the Challenge/Response protocol.

Figure 7 is an illustrative embodiment of the operations for configuring the token to provide security against the unauthorized access of the node.

user 130. The token 120 may be constructed in any form, preferably a form that is not too obtrusive to carry or wear. Examples of forms that can be used by the tokens include, but are not limited to pagers or identification badges. The function may also be implemented in another device with an alternative purpose such as a cellular telephone. The personal computer 110 periodically attempts to establish a communication link 140, represented by dotted lines, with the token 120 through infra-red ("IR") transmissions or through any other medium that does not require physical connection (e.g., radio frequency "RF" signals in which the personal computer 110 may require an antenna). The communication link 140 may be established and maintained only when the token 120 is within a predetermined distance (e.g., within 20 feet) from the personal computer 110. It is contemplated that although the wireless authentication system is being described with a personal computer, it could be implemented to secure any node being an electronic product such as a peripheral to the computer (printer, mass storage device, etc.), door locking mechanisms (i.e., garage door opener, electronic door locks) and the like.

Upon establishing the communication link 140, information is exchanged, normally in an encrypted format in at least one direction, between the security device (not shown) and the token 120. Upon the security device determining that the token 120 responded correctly, the user 130 is granted access to the contents (i.e., data, applications and other information stored thereon) of the personal computer 110 as well as its networked resources.

It is contemplated that the wireless authentication system 100 may be utilized with another authentication system (password-based system, card-based system, etc.) to prevent the personal computer 110 from being mistakenly accessed in certain situations. One situation is where the authorized user 130 wearing the token 120 is walking by the

The I/O subsystem 260 includes an I/O controller 265 which is coupled to both the first bus 200 and a second bus 270 (e.g., a Peripheral Component Interconnect "PCI" bus, Industry Standard Architecture "ISA" bus and the like). The I/O controller 265 provides a communication path to allow devices connected to the first bus 200 or the second bus 270 to exchange information. The second bus 270 allows information to be transferred from or to at least one peripheral device including, but not limited to a display device 275 (e.g., cathode ray tube, liquid crystal display, etc.); an alphanumeric input device 276 (e.g., an alphanumeric keyboard, etc.) for communicating information (address, data and control) to the host processor 225; a cursor control device 277 (e.g., a mouse, trackball, joystick, touchpad, etc.); a mass data storage device 278 (e.g., magnetic tapes, hard disk drive, floppy disk drive, etc.); an information transceiver device 279 (fax machine, modem, etc.) for transmitting information from the personal computer 110 to another remotely located device and for receiving information therefrom; and a hard copy device 280 (e.g., plotter, printer, etc.) for providing a tangible, visual representation of the information. It is contemplated that the personal computer shown in Figure 2 may employ some or all of these devices or different devices than those illustrated. For example, the security device 210 could be coupled to the second bus 270 instead of the first bus 200, a local bus (not shown) within the host processor 225 or may be adapted to any bus line coupling any of the peripheral devices such as the mass storage device 278.

Alternatively, the security device could be utilized for access control purposes outside the computer field such as in the automatic field, home and business security field. It is contemplated that the security device and token combination could be used to authenticate the holder of the token before granting access to a node of transportation (car, bus, farm equipment, etc.) garage, and home or office or any other node by implementing the security device in that

computer or its controlling node. It is an option for the token 120 to provide an on-board power source 330 (e.g., a battery) to possibly supply power to components within the token 120 for operational purposes as well as to possibly service the memory element 320 if needed. For some protocol implementations, inclusion of a random number generator may be desirable (particularly where the token is also used to authenticate the personal computer).

Referring to Figure 5, the operational steps performed by the wireless authentication system in periodically exchanging Challenge and Response messages between a node (e.g., computer, locking mechanism for car doors, home or office door entry, etc.) and the token is illustrated. In this embodiment, the node prompts a user for a password but continues to deny access to its contents and networked resources (Steps 400-405). Upon the user entering his or her password, the node determines whether the password is correct (Step 410). If the password is incorrect, the node prompts the user to re-enter the password. Of course, the node may be configured to allow only one or more tries to enter the password before precluding access to the node without assistance by security (such as a corporate security officer) or imposing a time-delay before one can attempt to try to access the node.

Alternatively, if the password is correct, the node, namely the security device, generates a Challenge message and transmits the Challenge message covering a predetermined distal range from the node (Step 415). Thereafter, it awaits a Response message from the token and its verification before allowing the user access to the content stored on the node or its networked resources (Step 420). If no Response message is received after a prescribed period of time, access is denied (Step 425). Otherwise, upon receiving the Response message, the node verifies whether the Response message is correct (Step 430). If the Response message is incorrect, the user is denied access to the node by any conventional manner such as by displaying a screen-obscuring image, refusing further input from the keyboard,

equivalent. If so, the user is provided access to the data stored within the node and if not, the user is prevented such access.

Another illustrative example is shown in Figure 6C where the security device 210 is not designed to store any public keys associated with authorized tokens. As a result, a digital certificate is required as shown. The security device 210 transmits a random number ("RN") 540 to the token 120. The token 120 receives RN 540 and encrypts RN 540 with the private key of the token "PRT" to produce an encrypted random number "RN_{prt}" 545 as part of a Response message 550. The other part of the Response message 550 is a digital certificate 555 obtained from a well-known Trusted Authority 560 (e.g., system administrator, company security, etc.) in which its public key "PUTA" 565 is widely disseminated. The digital certificate 555 is the public key of the token ("PUT") 575 encrypted with the private key of the Trusted Authority "PRTA" 570. Both parts of the Response message 550 are transmitted to the security device 210.

Upon receiving the Response message 550, the security device 210 decrypts the digital certificate 555 with PUTA 565 to obtain PUT 575. Next, PUT 575 is used to decrypt RN_{prt} 545. Finally, RN 580 received from the token is compared to RN 540 transmitted to the token 120 and if these numbers are equivalent, the Response message 550 is correct.

Alternatively, in lieu of a password-based system being implemented within the node, the token may be configured to require a password or a personal identification number ("PIN"). Thus, the token remains in an inactive state unless its user periodically authenticates himself or herself. Of course, the advantage of having the password-based system employed within the node is that the node is already adapted with I/O devices (e.g., an alphanumeric keyboard) to assist a user in authenticating himself or herself. However, as stated previously, the node is susceptible to virus attacks which would not be an issue if the password-based system is employed within the token.

node awaits a Response message within a prescribed time period. If the node does not receive a Response message within that time or receives an incorrect Response message, access is denied to the node (Steps 635-645). However, if the node receives the Response message within the prescribed period of time and it is correct, the user is granted access to the node (Step 650).

Thereafter, timing circuitry within the node is set for the node to generate another Challenge message after a predetermined time period has expired (Step 655). Next, the token is checked to see whether it has been in the active state for longer than the selected time (Step 660). If so, the token becomes nonfunctional and the user is denied access to the node (Step 665). If the token is still active, the timing circuitry of the node is checked to see whether the predetermined time period has expired (Step 670). If not, the state of the token and expiration of the time period set by the timing circuitry in the node is checked at a later time. Otherwise, if the timing period has expired, the node is prompted to generate another Challenge message to the token for periodic authentication that the user is proximate to the node.

While various embodiments of the invention have been described, those skilled in the art will realize that other embodiments of the invention are easily foreseeable without departing from the spirit and scope of the present invention. For example, the token may initiate query messages to allow the node to determine when the token is in the proximity. Likewise, the periodic challenge/response communications may be initiated by the token rather than the node so long as the node still authenticates the token. Moreover, well known circuitry and operational steps are not set forth in detail in order to avoid unnecessarily obscuring the present invention. The invention should, therefore, be measured in terms of the following claims.

5. The method according to claim 1, wherein said first message includes a random number and said second message correctly responds to said first message by returning said random number.

6. The method according to claim 5, wherein said first message includes said random number in a non-encrypted format and said second message includes said random number encrypted with a private key associated with the token.

7. The method according to claim 5, wherein said first message includes said random number encrypted with a public key associated with the token and said second message includes said random number in a non-encrypted format.

8. The method according to claim 5, wherein said first message includes said random number and said second message includes said random number encrypted with a private key associated with the token and a digital certificate containing a public key associated with the token encrypted with a private key of a trusted authority.

9. The method according to claim 1, wherein said periodicity of said first and second message exchanges is programmable.

10. The method according to claim 1, wherein prior to step (a), the method comprises the steps of:

transferring a query message from the node to the token; and

transferring a response to the node by the token when the token is within said predetermined distance from the node.

14. The method according to claim 12, wherein prior to step (c), the method further comprises the steps of

transferring query message from the token to the node; and

transferring a response message from the node to the token indicating that the node acknowledges that the token is within the predetermined distance.

15. A wireless authentication system to control an operating state of a first node having at least a first data bus to support communications internally within the first node based on the proximity of an authorized user possessing a token to the first node, the wireless authentication system comprising:

a security device implemented within the first node having a wireless transceiver, said security device generating a plurality of messages to be transmitted to the token through said wireless transceiver, wherein each of said plurality of messages is separately transmitted after a prescribed time interval has elapsed; and

the token that establishes a wireless communication link with said security device, wherein said security device and said token operate to place the first node in an operational state using said plurality of messages.

16. The wireless authentication system of claim 15, wherein each of said plurality of messages generated by said security device is separately transmitted after a prescribed time interval has elapsed.

17. The wireless authentication system according to claim 16, wherein the token (i) initially receives a first message of said plurality of messages, (ii) generates a message in response to said first message for transmission to said security device to place the first node in said operational state and (iii) generates a message in response to each of

21. The wireless authentication system according to claim 20, wherein said token further includes a power source to provide power to at least said memory element and said processor.

22. The wireless authentication system according to claim 17, wherein said first message includes a random number and said second message correctly responds to said first message by returning said random number.

23. The wireless authentication system according to claim 17, wherein said first message includes said random number in a non-encrypted format and said second message includes said random number encrypted with a private key associated with the token.

24. The wireless authentication system according to claim 17, wherein said first message includes said random number encrypted with a public key associated with the token and said second message includes said random number in a non-encrypted format.

25. The wireless authentication system according to claim 17, wherein said first message includes said random number and said second message includes said random number encrypted with a private key associated with the token and a digital certificate containing a public key associated with the token encrypted with a private key of a trusted authority.

26. The wireless authentication system according to claim 15, wherein the node is one of a computer and a door control mechanism.

27. A wireless authentication system to control an operating state of a first node based on the proximity of an authorized user to the

29. The wireless authentication system according to claim 28, wherein said token means includes

second bus means for providing a data path within said token means;

said second interface means for receiving said plurality of messages and for transmitting a corresponding plurality of messages in response to said plurality of messages, said second interface means being coupled to said second bus means and to said first interface means of said security means through the communication link;

second memory means for storing cryptographic information, said second memory means being coupled to said second bus means; and

second processor means for generating said corresponding plurality of messages in response to said plurality of messages, said second processor means being coupled to said second bus means.

30. The wireless authentication system according to claim 29, wherein said token means further includes power means for providing power to at least said second memory means and said second processor means.

31. The wireless authentication system according to claim 27, wherein said first message includes a random number and said second message correctly responds to said first message by returning said random number.

32. The wireless authentication system according to claim 27, wherein said first message includes said random number in a non-encrypted format and said second message includes said random number encrypted with a private key associated with the token means.

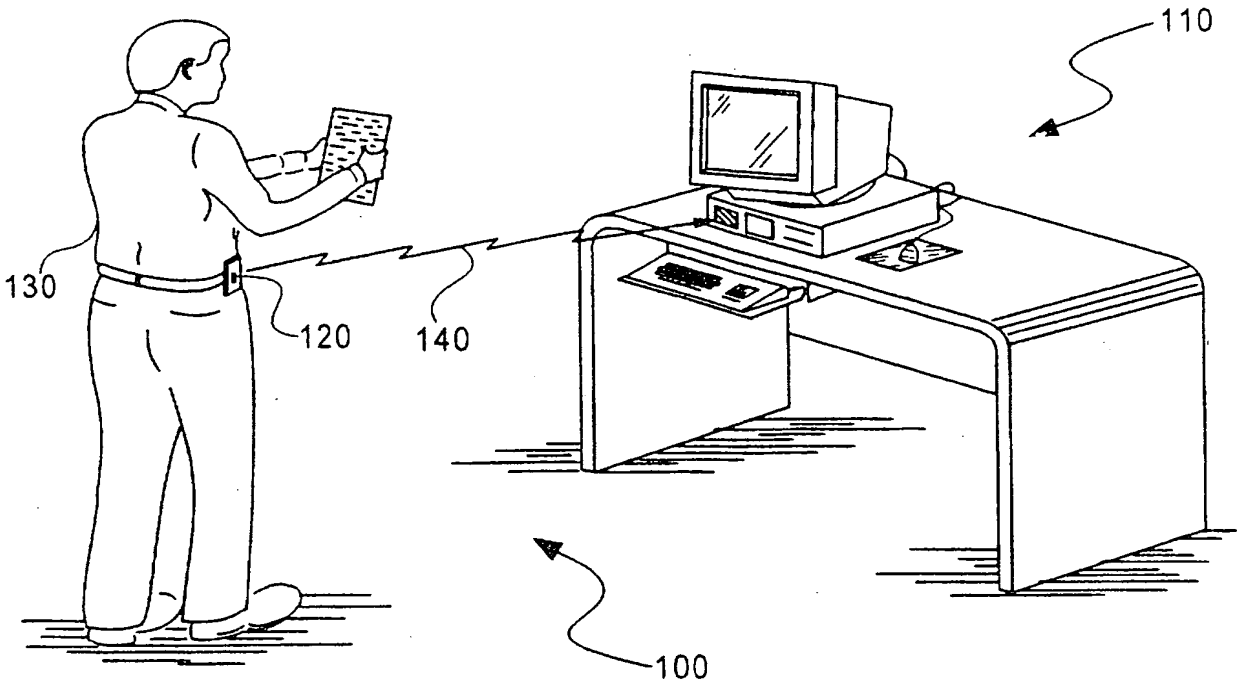


FIG. 1

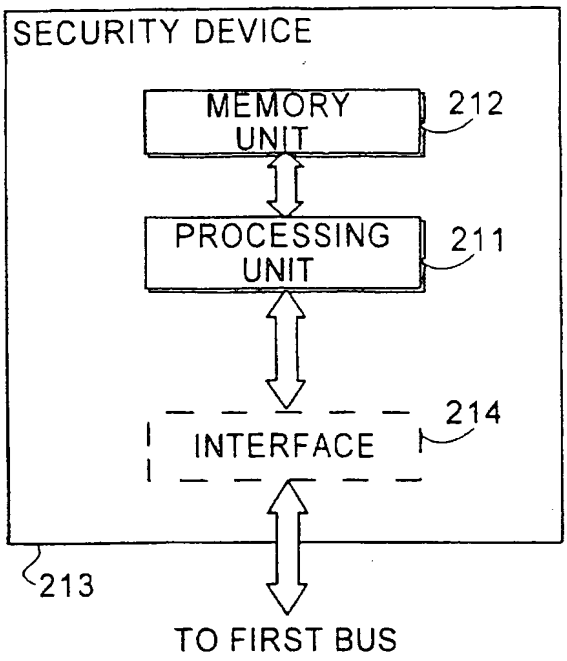


FIG. 3

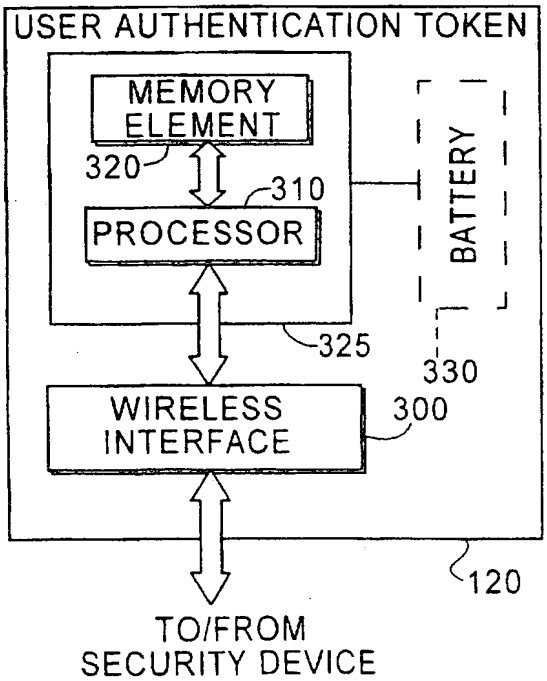


FIG. 4

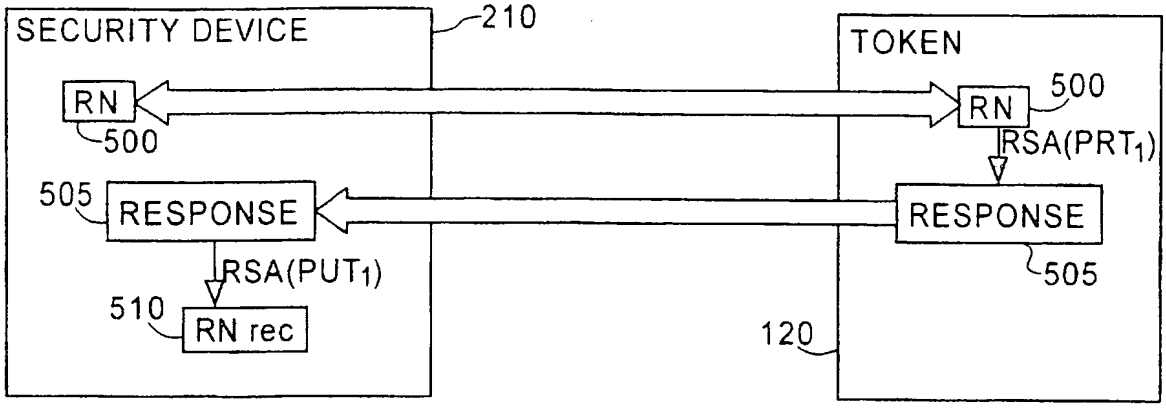


FIG. 6A

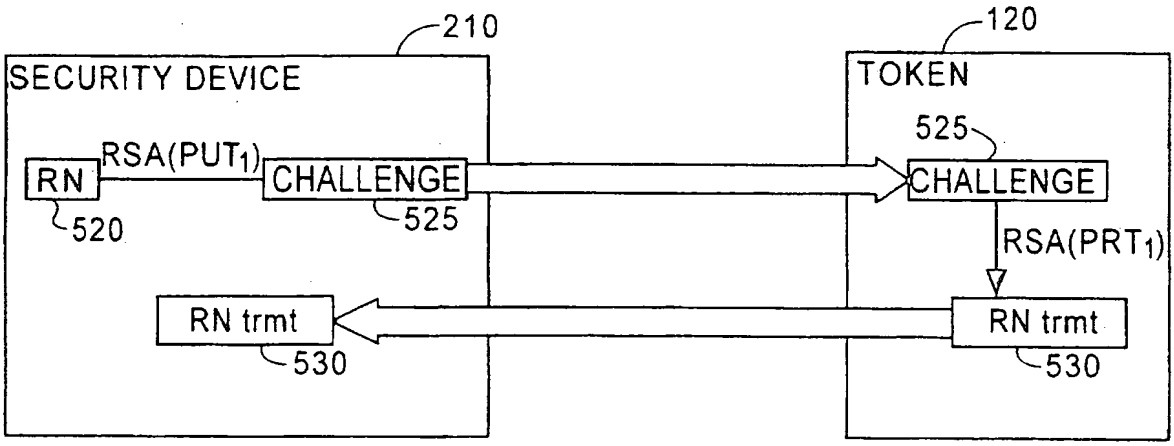


FIG. 6B

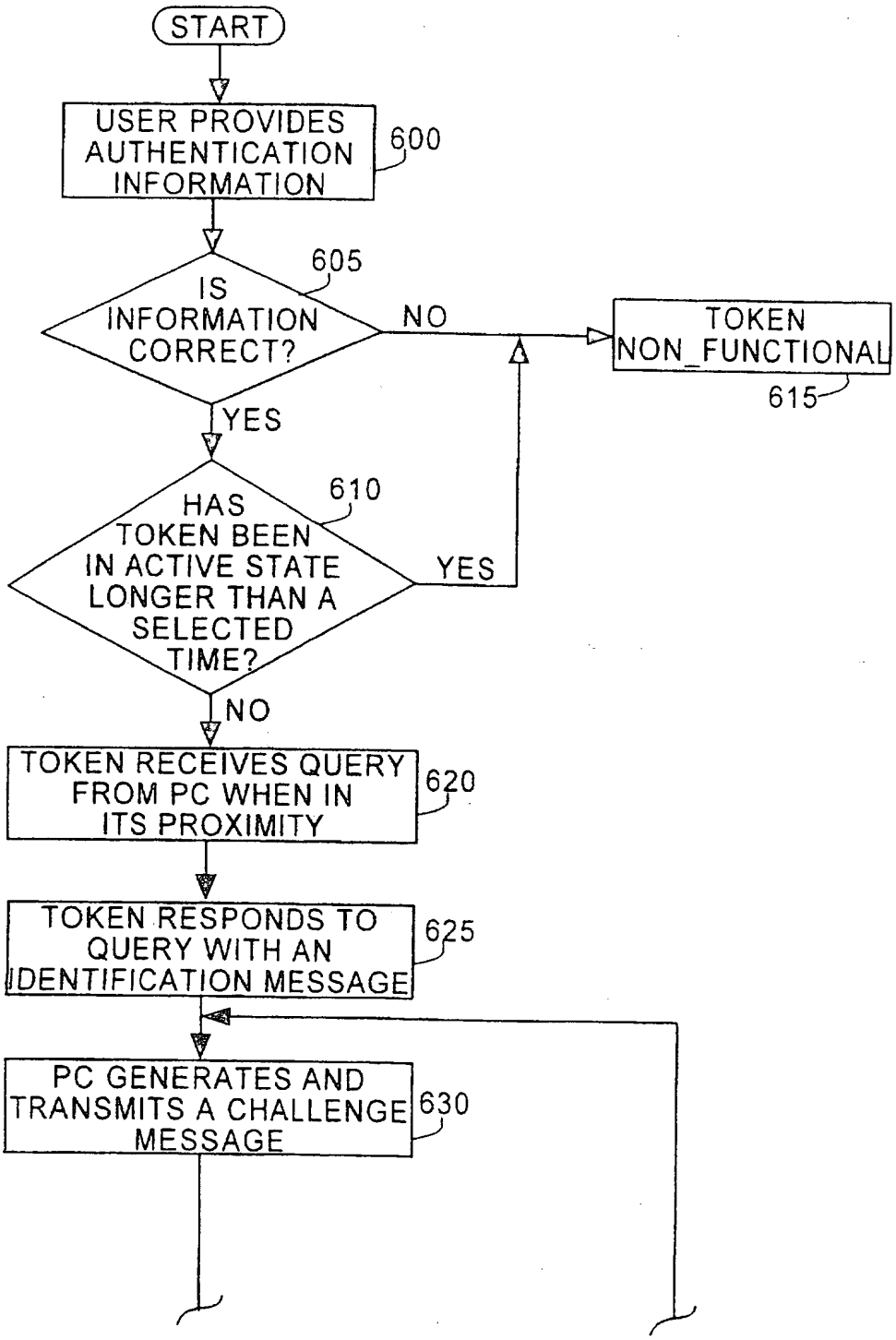


FIG. 7A

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/04025

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04L 9/32;
US CL : 380//23, 25; 340/825.31
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380//23, 25; 340/825.31

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS: search terms-authenticate, transponder, periodic, random number, certificate

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,097,505 A (WEISS) 17 March 1992, column 2, lines 38-53; column 3, lines 58-61; column 7, lines 6-16; column 9, lines 51-67.	1-4, 9-18, 20-30
Y	US 5,144,667 A (POGUE, JR. ET AL) 01 September 1992, column 5, lines 9-30; column 3, line 58- column 4, line 39.	5-7, 22-24, 32, 33
X	US 5,131,038 A (PUHL ET AL) 14 July 1992, column 4, lines 5-24.	1-4, 9-18, 20, 26-29
A	US 5,432,851 A (SCHEIDT ET AL) 11 July 1995, column 3, lines 22-50.	1, 12, 15, 27
A	US 5,280,527 A (GULLMAN ET AL) 18 January 1994, column 2, lines 30-39.	1, 12, 15, 27

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 JUNE 1997	11 JUL 1997

Name and mailing address of the ISA/US	Authorized officer
Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	GILBERTO BARRÓN
Facsimile No. (703) 305-3230	Telephone No. (703) 306-4177

Form PCT/ISA/210 (second sheet)(July 1992)*